For favour of posting

DEPARTMENT OF STATISTICS AND ACTUARIAL SCIENCE
THE UNIVERSITY OF HONG KONG

Departmental Seminar

Dr. Jun ZHAO

School of Computer Science and Engineering
Nanyang Technological University
Singapore

will give a talk

entitled

THEORETICAL APPROACHES TO PRIVACY AND SECURITY ISSUES IN DATA ANALYTICS AND NETWORKED SYSTEMS

Abstract

Technologies for data analytics and networked systems pose privacy and security issues while providing ever-smarter services. To address these issues, my work takes theoretical approaches and leverages tools from probabilistic graphical models, graph theory, and cryptography.

About privacy and security in data analytics, I will first present my current research on deep learning under differential privacy, where differential privacy by Dwork et al. provides a theoretical framework to quantify privacy. Differentially private algorithms generate noisy answers to protect sensitive data. Under the iterative process of stochastic gradient descent in deep learning, my approach reuses a fraction of the noise added to the gradient in earlier iterations for later iterations. The result improves the tradeoff between privacy and learning accuracy over prior work. Afterwards, I will introduce my mechanisms for differential privacy under correlated data, by analyzing tuples' dependency structures in the form of probabilistic graphical models. I further apply the mechanisms to adaptive data analysis with correlated samples, where the testing dataset is reused and the estimates evaluated on the testing dataset can be chosen adaptively based on the results of prior estimates. In addition, I will outline future directions in attack-resilient data analytics. In particular, one goal is to prevent maliciously crafted samples from triggering misbehavior of machine learning systems.

About security in networked systems, I will first review my extensive studies which apply graph theory to security in sensor networks employing key predistribution schemes. Then I will talk about my research of designing cryptographic functions for updating a secret pool on an embedded device in order to achieve remote device authentication. Moreover, I will discuss future work on using graph theory to design resilient cyber-physical systems.

on

Thursday, March 8, 2018

(Refreshments will be served from 2:15 p.m. outside Room 301 Run Run Shaw Building)

2:30 p.m. – 3:30 p.m.

at

Room 301, Run Run Shaw Building

Visitors Please Note that the University has limited parking space. If you are driving please call the Department at 3917 2466 for parking arrangement.

All interested are welcome